GREENBERG TRAURIG, LLP
Ian C. Ballon (SBN 141819)
Ballon@gtlaw.com
1900 University Avenue, 5th Floor
East Palo Alto, CA 94303
Tel.: 650-328-8500
Fax: 650-328-8508

Lori Chang (SBN 228142)
ChangL@gtlaw.com
Rebekah S. Guyon (SBN 291037)
GuyonR@gtlaw.com
1840 Century Park East, 19th Floor
Los Angeles, CA 90067-2121
Tel: 310-586-7700
Fax: 310-586-7800

Attorneys for Defendants
Slice Technologies, Inc. and
Unrollme Inc.

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

JASON COOPER, individually and on behalf of all others similar situated,

Plaintiff,

v.

SLICE TECHNOLOGIES, INC., a Delaware corporation, and UNROLLME INC., a Delaware corporation,

Defendants.

Case No. 17-cv-02340-LB

DEFENDANTS SLICE TECHNOLOGIES, INC. AND UNROLLME INC.'S NOTICE OF MOTION AND MOTION TO DISMISS PURSUANT TO FED. R. CIV. PROC. 12(B)(1) AND 12(B)(6); MEMORANDUM OF POINTS AND AUTHORITIES

Hearing date: July 27, 2017
Time: 9:30 a.m.

Complaint filed: April 26, 2017

TABLE OF CONTENTS

Page

NOTICE OF MOTION AND MOTION TO DISMISS 1

MEMORANDUM OF POINTS AND AUTHORITIES 2

I. INTRODUCTION 2

STATEMENT OF ISSUES TO BE DECIDED 4

II. PLAINTIFF'S ALLEGATIONS 5

A. Unrollme Provides A Free Email Management Service 5

B. Plaintiff Argues That Unrollme's Privacy Policy Is "Deficient" But The Challenged Business Practices Are Explained In The Privacy Disclosures 5

C. Plaintiff Does Not Allege Actual Harm Or Injury 7

III. ARGUMENT 7

A. The Complaint Should Be Dismissed In Its Entirety Because Plaintiff Does Not Establish An Injury In Fact (Fed. R. Civ. Proc. 12(b)(1)) 7

1. Plaintiff Does Not Allege An Injury In Fact 8

2. Any Potential Future Harm That Plaintiff Alleges Is Purely Speculative 12

B. Plaintiff's Claims Should Be Dismissed Under Fed. R. Civ. Proc. 12(b)(6) 14

1. Plaintiff Cannot State A Claim Under The Wiretap Act Or SCA Because Unrollme Is A Party And/Or Intended Recipient Of His Messages 14

2. Cooper Does Not Allege A Plausible "Interception" Under The Wiretap Act 17

IV. CONCLUSION 19

TABLE OF AUTHORITIES

Page(s)

Federal Cases

In re American Airlines, Inc. Privacy Litigation,
370 F. Supp. 2d 552 (N.D. Tex. 2005) 17

Antman v. Uber Techs., Inc.,
No. 3:15-cv-01175-LB, 2015 WL 6123054 (N.D. Cal. Oct. 19, 2015) 12

Ashcroft v. Iqbal,
556 U.S. 662 (2009) 14

Atlantic Marine Const. Co. v. U.S. Dist. Ct. for the W. Dist. of Tex.,
134 S. Ct. 568 (2013) 8

Attias v. CareFirst, Inc.,
199 F. Supp. 3d 193 (D.D.C. 2016) 13

Bell Atl. Corp. v. Twombly,
550 U.S. 544 (2007) 14

Cahen v. Toyota Motor Corp.,
147 F. Supp. 3d 955 (N.D. Cal. 2015) 13

Caro v. Weintraub,
618 F.3d 94 (2d Cir. 2010) 15, 16

Clapper v. Amnesty Int'l,
133 S. Ct. 1138 (2013) 4, 12

Cruper-Weinmann v. Paris Baguette Am., Inc.,
__F. Supp. 3d__, 2017 WL 398657 (S.D.N.Y. Jan.30, 2017) 8, 10, 12

In re DoubleClick Inc. Privacy Litig.,
154 F. Supp. 2d 497 (S.D.N.Y. 2001) 15, 16, 17

In re Facebook Privacy Litig.,
791 F. Supp. 2d 705 (N.D. Cal. 2011)) 17

Fero v. Excellus Health Plan, Inc.,
__F. Supp. 3d__, No. 6:15-CV-06569 EAW, 2017 WL 713660 (W.D.N.Y. 2017) 13

Gaos v. Google, Inc.,
No C 10-04809 JW, 2011 WL 7295480 (N.D. Cal. Apr. 7, 2011) 10, 11

In re Google Inc. Cookie Placement Consumer Privacy Litig.,
806 F.3d 125 (3d Cir. 2015) 15, 16

Hoyle v. Diamond,
No. 08-cv-347C, 2013 WL 1152037 (W.D.N.Y. Mar. 19, 2013) 18

Konop v. Hawaiian Airlines, Inc.,
302 F.3d 868 (9th Cir. 2002) 17, 18

Low v. LinkedIn Corp.,
No. 11-CV-01468-LHK, 2011 WL 5509848 (N.D. Cal. Nov. 11, 2011) 10

Lujan v. Defenders of Wildlife,
504 U.S. 555 (1992) 7, 8

Mintz v. Mark Bartelstein & Assocs. Inc.,
906 F. Supp. 2d 1017 (C.D. Cal. 2012) 18

In re Nickelodeon Consumer Privacy Litig.,
827 F.3d 262 (3d Cir. 2016) 16

Spokeo, Inc. v. Robbins,
136 S. Ct. 1540 (2016) 3, 7, 8

Steve Jackson Games, Inc. v. U.S. Secret Serv.,
36 F.3d 457 (5th Cir. 1994) 18

Theofel v. Farey-Jones,
359 F.3d 1066 (9th Cir. 2004) 18

Vigil v. Take-Two Interactive Software, Inc.,
__F. Supp. 3d__, 2017 WL 398404 (S.D.N.Y. Jan. 30, 2017) 10, 11, 13

Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.,
829 F.3d 197 (2d Cir. 2016) 18

Whalen v. Michaels Stores, Inc.,
__F. App'x __, 2017 WL 1556116 (2d Cir. May 2, 2017) 9, 10, 11, 12

In re Zynga Privacy Litig.,
No. C 10-04680 JWW, 2011 WL 7479170 (N.D. Cal. June 15, 2011) 17

Federal Statutes

15 U.S.C. § 7702 6

18 U.S.C. § 2510(4) 17

18 U.S.C. § 2510(12) 14

18 U.S.C. § 2511 17

18 U.S.C. § 2511(2)(d) 4, 14, 15, 16

18 U.S.C. § 2701(c)(2) 4, 14, 15

18 U.S.C. § 2702(b)(1) 4, 17

18 U.S.C. § 2702(b)(3) 17

28 U.S.C. § 2510 2

28 U.S.C. § 2701 2

State Statutes

740 Ill. Comp. Stat. § 14/1 10

Rules

Fed. R. Civ. P. 12(b)(1) 1, 4, 7, 19
Fed. R. Civ. P. 12(b)(6) 1, 4, 14, 19

Other Authorities

Mike Isaac and Steve Lohr, *Unroll.me Service Faces Backlash Over a Widespread Practice: Selling User Data*, N.Y. Times, April 24, 2017 3
S. Rep. No. 99-541 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555 11

NOTICE OF MOTION AND MOTION TO DISMISS

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that on July 27, 2017 at 9:30 a.m., or as soon thereafter as the matter may be heard, before the Honorable Laurel Beeler, Courtroom C of the United States District Court for the Northern District of California, located at 450 Golden Gate Avenue, 19th Floor, San Francisco, CA 94102, defendants Slice Technologies, Inc. and Unrollme Inc. will and hereby do respectfully move for an order dismissing plaintiff's complaint in its entirety pursuant to Fed. R. Civ. Proc. 12(b)(1) and 12(b)(6).

This motion is based on this Notice of Motion and Motion, the Memorandum of Points and Authorities in support thereof, all pleadings and papers on file in this action, and such other written or oral argument as may be properly presented to the Court at the hearing.

Respectfully submitted,

DATED: June 19, 2017

GREENBERG TRAURIG, LLP

By: */s/ Ian C. Ballon*
Ian C. Ballon
Lori Chang
Rebekah S. Guyon
Attorneys for defendants Slice Technologies, Inc. and Unrollme Inc.

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Plaintiff Jason Cooper filed suit based on the theoretical possibility, unsupported by anything more than conjecture (not facts), that aggregated anonymized data potentially could be de-anonymized to identify individual users whose emails were allegedly accessed and "data mined" by defendants Unrollme Inc. and Slice Technologies, Inc. *See* Compl. ¶¶ 31-33. Unrollme offers a free web-based "email management" service that helps users "clean up" their email inboxes by "easily unsubscrib[ing] [users] from mailing lists, newsletters and other annoying emails." Compl. ¶¶ 2-3. Its parent company Slice collects data "using 'technology that automatically identifies e-receipts within [email] inboxes'" and extracts data from them about purchases made via online shopping. *Id.* ¶ 15. Plaintiff signed up to use Unrollme's services and gave Unrollme "permission" to "access" his Gmail account to "[r]ead, send, delete, and manage [his] email" upon account creation and "continu[ing] into the future." *Id.* ¶¶ 20-22, 35, 38. Plaintiff now asserts violations of Title I and Title II of the Electronic Communications Privacy Act ("ECPA"), 28 U.S.C. §§ 2510 *et seq.* and §§ 2701 *et seq.*, based on the factually unsupported and conclusory allegations that Unrollme and Slice intercepted and accessed his emails without consent or authorization, or otherwise exceeded authorization by allegedly "accessing emails for purposes other than the identification of 'subscription' emails." Compl. ¶¶ 53, 56, 59, 61. The crux of plaintiff's complaint is the allegation that "UnrollMe hides the fact that it actually scours your email for valuable data and then sells that through its parent company, Slice." *Id.* ¶ 29. Contrary to plaintiff's allegation, defendants do not in fact "sell" actual emails collected from Unrollme "to anyone willing to pay," including companies like Uber.[1] *See id.* ¶ 34.

[1] Plaintiff's allegation that *The New York Times* reported in an article by Mike Isaac that Slice Intelligence sold "private emails" of Unrollme users to Uber is completely false. The article itself, incorporated by reference in the complaint (*id.* ¶ 25) and posted at https://www.nytimes.com/2017/04/23/technology/travis-kalanick-pushes-uber-and-himself-to-the-precipice.html?_r=0, focuses on Uber's activities, and states in brief that "[u]sing an email digest service it owns named Unroll.me, Slice collected its customers' emailed Lyft receipts from their inboxes and sold the *anonymized data* to Uber" (emphasis added). A subsequent article by Mr. Isaac, linked from this article, makes clear that

> What Unroll.me does is far from an anomaly—it is part of an expansive and largely unregulated world of selling personal data collected by online consumer services. As

But even that were true (and it is not), plaintiff's assertion that these purported business practices were not "adequately" disclosed is belied by Unrollme's Privacy Policy, which users must assent to, and which candidly explains that data from users' "commercial" and "transactional" messages (namely, e-receipts), and the messages themselves, may be collected for the express purpose of understanding customer behavior, disclosed and sold with personal information removed, and used "to build anonymous market research products and services with trusted business partners." *See id.* ¶¶ 4, 19, 28. Taking these disclosures at face value, they defeat plaintiff's claims that defendants accessed users' emails without authorization.

First, plaintiff fails to allege any facts that establish his standing to sue. Plaintiff concedes that Unrollme had authorization to access his emails to perform the free email management services he signed up for. While he contends that he suffered an injury to his privacy interest because he purportedly was not "informed" that data from emails was being collected to build aggregated anonymized market research products (notwithstanding the clear disclosures in the Privacy Policy), he has not alleged any economic harm or other injury arising out of the collection and/or sale of aggregated anonymized data, and therefore fails to allege any facts to show that he suffered a "concrete" injury to support standing under Article III. *Spokeo, Inc. v. Robbins*, 136 S. Ct. 1540, 1548 (2016). While plaintiff asserts in the abstract that anonymized data has the *possibility* to be de-anonymized by companies like Uber, he does not allege that any anonymized data extracted from his emails in fact was re-identified, let alone re-identified by these defendants. Merely hypothetical concerns of future harm are too speculative to arise to the status of a "certainly impending" injury to

---

> long as a service like Unroll.me has a privacy policy, adheres to it and does not sell personally identifiable information, like someone's name, it is fairly free to package and sell the data it collects. . . .

The article goes on to explain that Unrollme discloses its

> use of personal data in its privacy policy, which says that "we may collect, use, transfer, sell and disclose nonpersonal information purpose" and that the data can be used "to build anonymous market research products and services."

Mike Isaac and Steve Lohr, *Unroll.me Service Faces Backlash Over a Widespread Practice: Selling User Data*, N.Y. Times, April 24, 2017, https://www.nytimes.com/2017/04/24/technology/personal-data-firm-slice-unroll-me-backlash-uber.html.

support standing. *Clapper v. Amnesty Int'l*, 133 S. Ct. 1138, 1147 (2013). His claims should therefore be dismissed in their entirety under Fed. R. Civ. P. 12(b)(1).

Second, plaintiff fails to state a claim under either Title I or Title II of ECPA because plaintiff assented to the broad disclosures in the Privacy Policy, authorized access to his Gmail account, and therefore made defendants a "party" to and an "intended recipient" of his electronic communications. The Wiretap Act (Title I) excludes from liability an interception by a "party to the communication or where one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(d). The Stored Communications Act ("SCA") (Title II) excludes from liability the access of a stored electronic communication "by a user of [an electronic communication service] with respect to a communication of or intended for that user," 18 U.S.C. § 2701(c)(2), and the disclosure of the contents of an electronic communication to an "addressee or intended recipient of such communication, or an agent of such addressee or intended recipient," or "with the lawful consent of the originator or an addressee or intended recipient of such communication," 18 U.S.C. § 2702(b)(1), (3). Courts construing these provisions have also held that a party or intended recipient of a communication authorized by a third party is not liable under ECPA. *See* Section III(B)(1), *infra*.

In addition, plaintiff fails to allege any facts to show that defendants "intercepted" an electronic communication in order to state a claim under the Wiretap Act, where plaintiff's claim rests on allegations that defendants accessed his stored emails in his Gmail account. Because the Wiretap Act does not apply to communications in storage, plaintiff cannot state a claim under Title I of ECPA, which is subject to dismissal under Fed. R. Civ. Proc. 12(b)(6).

Dismissal is therefore warranted under either Rule 12(b)(1) or Rule 12(b)(6), or both.

STATEMENT OF ISSUES TO BE DECIDED

Whether the Court should dismiss plaintiff's complaint with prejudice (1) pursuant to Fed. R. Civ. P. 12(b)(1) for failure to allege an injury in fact sufficient to confer Article III standing; or (2) pursuant to Fed. R. Civ. P. 12(b)(6) for failure to state a claim (a) under either Title I or Title II of ECPA because Unrollme was either a party or an intended recipient of Cooper's electronic communications; and (b) under the Wiretap Act because Cooper has failed to allege a plausible interception; and (3) because Cooper cannot cure these deficiencies through amendment.

II. PLAINTIFF'S ALLEGATIONS

A. Unrollme Provides A Free Email Management Service

Unrollme offers a free web-based "email management" service that helps users "clean up" their email inboxes by allowing users "to easily unsubscribe from mailing lists, newsletters and other annoying emails." Compl. ¶¶ 2-3. Plaintiff alleges that "[b]y signing up with UnrollMe, consumers could purportedly rid their email inboxes of junk by allowing users to mass unsubscribe from spam messages and also by allowing them to group categories of emails into a single email digest that would be sent to the user daily." *Id.* ¶ 13.[2] To use this service, "users need to grant UnrollMe access to their email accounts (such as Gmail or Outlook) so that UnrollMe can identify and automatically unsubscribe them from any unwanted messages." *Id.* ¶ 3.

Plaintiff alleges that "once [UnrollMe] gets access to users' inboxes, it actually scans their emails, extracts a variety of data points, and then, through its parent company Defendant Slice Technologies, Inc. (doing business as Slice Intelligence), sells that data to third parties seeking to profile and target you." *Id.* "Slice gathers its data using 'technology that automatically identifies e-receipts within [email] inboxes, extract[ing] every data point about every purchase at the time level' from a 'panel' of online shoppers." *Id.* ¶ 15 (quoting Slice's website).

Plaintiff signed up to use Unrollme's services and gave Unrollme "permission" to "access" his Gmail account to "[r]ead, send, delete, and manage [his] email" upon account creation and "continu[ing] into the future." *Id.* ¶¶ 20-22, 35, 38.

B. Plaintiff Argues That Unrollme's Privacy Policy Is "Deficient" But The Challenged Business Practices Are Explained In The Privacy Disclosures

The core of plaintiff's complaint is that "Defendants did not adequately disclose to consumers the true purpose for why they seek access to UnrollMe users' emails for an important and obvious reason: few (if any) consumers would knowingly hand over complete access to their private emails to

[2] Plaintiff further alleges that "[i]n exchange, UnrollMe could display daily advertisements to users via the digests and offer them new productivity products or services over time," but this is a mischaracterization. *Id.* The digest (known as the "Rollup" feature) displays all email subscriptions (the ones the user chooses not to unsubscribe) in a single email sent to the user's inbox. The digest is a tool that organizes a user's email subscriptions for easy viewing. In any case, however, the allegation is irrelevant to plaintiff's claims or the pending motion.

a company that would invasively scour through them and then sell the data they gather about you to whoever would pay the most." *Id.* ¶ 4. But this is a policy argument, not a factual allegation, and is also disingenuous.

While plaintiff contends that "UnrollMe does not adequately disclose its true business model" (*id.* ¶ 17), the business practices that plaintiff challenges in this lawsuit are explained in Unrollme's Privacy Policy, which the complaint quotes as stating:

> We also collect non-personal information – data in a form that does not permit direct association with any specific individual. We may collect, use, transfer, sell, and disclose non-personal information for any purpose. For example, when you use our services, we may collect data from and about the "commercial electronic mail messages" and "transactional or relationship messages" (as such terms are defined in the CAN-SPAM Act (15 U.S.C. 7702 et. seq.) [sic] that are sent to your email accounts. **We collect such commercial transactional messages** so that we can better understand the behavior of the senders of such messages, and better understand our customer behavior and improve our products, services, and advertising. **We may disclose, distribute, transfer, and sell such messages and the data that we collect** from or in connection with such messages; provided, however, if we do disclose such messages or data, all personal information contained in such messages will be removed prior to any such disclosure.
>
> We may collect and use your commercial transactional messages and associated data **to build anonymous market research products and services with trusted business partners**.

Id. ¶ 28 (emphasis added).

Contrary to plaintiff's allegation that "UnrollMe hides the fact that it actually scours your email for valuable data and then sells that through its parent company, Slice" (*id.* ¶ 29), the privacy disclosures above clearly and expressly state in no uncertain terms that Unrollme accesses and collects users' messages and the data from them, may use such data to build anonymized market research products with "trusted business parties" (which plaintiff alleges is its own parent company, Slice), and may disclose, distribute, transfer, or sell such messages and data to third parties (which plaintiff alleges includes Uber, *see id.* ¶ 25).

Plaintiff also argues that the Privacy Policy is "deficient" and "inconsistent with UnrollMe's marketing materials and representations about what the service is and why consumers should sign up for it." *Id.* ¶ 29. However, the allegation that "UnrollMe heavily emphasizes throughout its marketing materials and website . . . that it needs access to users' email accounts *specifically* to search for

subscription emails that UnrollMe can assist in unsubscribing from" is not contrary to or refuted by the privacy disclosures. *Id.* (italics in original).

C. Plaintiff Does Not Allege Actual Harm Or Injury

Nowhere in plaintiff's complaint does he allege facts showing he was actually harmed by the purported deficiencies in Unrollme's Privacy Policy and/or marketing materials. Plaintiff alleges that unnamed "consumers" who register to use Unrollme's services allegedly "had their privacy and trust violated" (*id.* ¶ 34), but he does not allege that *he* suffered any economic loss or actual damage caused by defendants' alleged conduct.

Rather, plaintiff's complaint is predicated on the mere possibility of an abstract risk of harm, not supported by any facts, based on mere speculation and conjecture. Plaintiff alleges that "[e]ven assuming Defendants performed *some* level of anonymization (*e.g.*, removing first and last names and email addresses), it *likely* wasn't sufficient. Time and time again, researchers have revealed the ease in which they can identify particular people from purportedly anonymized data sources." *Id.* ¶ 31 (emphasis added). Regarding Lyft email receipts, plaintiff posits that "even if Defendants attempted some anonymization technique, they *may* have overlooked information unique to the consumer." *Id.* ¶ 32 (emphasis added). Further, plaintiff alleges that based on "[t]he reputation of Uber, the company Defendants sold consumers' email data to," and "[g]iven Uber's reported proclivity for invasive tracking, it *likely* has the means to re-identify the Lyft data Defendants sold to it." *Id.* ¶ 34 (emphasis added). These are all hypothetical assertions—none of which constitute facts or proof that plaintiff was actually or imminently harmed by defendants' alleged conduct. Indeed, plaintiff does not even allege that he was a Lyft user during the time he was using Unrollme's email management services.

III. ARGUMENT

A. The Complaint Should Be Dismissed In Its Entirety Because Plaintiff Does Not Establish An Injury In Fact (Fed. R. Civ. Proc. 12(b)(1))

Article III requires that "plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016) (citing *Lujan v.*

Defenders of Wildlife, 504 U.S. 555, 560-61 (1992)).[3] An "injury in fact" requires both a "concrete" and a "particularized" harm, which must be "actual or imminent, not conjectural or hypothetical." *Spokeo*, 136 S. Ct. at 1548. "For an injury to be 'particularized,' it must affect the plaintiff in a personal and individual way." *Spokeo*, 136 S. Ct. at 1548. A "concrete" injury "must be 'de facto'; that is, it must actually exist." *Id*. ("When we have used the adjective 'concrete,' we have meant to convey the usual meaning of the term—'real,' and not 'abstract.'"). Although a "concrete" injury may be intangible, whether an intangible harm constitutes an injury in fact must be "grounded in historical practice," and *Spokeo* instructs courts "to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." *Id*. at 1549. However, "even in the context of a statutory violation," a plaintiff cannot "allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III." *Id*. Standing, therefore requires a plaintiff to identify and demonstrate an actual, concrete harm that is particularized and distinct from merely showing that a defendant violated some statutory right of the plaintiff. Courts following *Spokeo* have reinforced this standard:

> [T]o determine whether a procedural violation alone constitutes an injury in fact, a court must inquire (1) whether Congress conferred the procedural right at issue in order to protect a concrete interest of the plaintiff, and (2) whether the violation of the procedure at issue presented a material risk of harm to that interest. A plaintiff may fail to satisfy the second condition when the violation in question could not result in harm to the interest protected by statute either as a general matter . . . , or under the particular circumstances alleged . . . .

Cruper-Weinmann v. Paris Baguette Am., Inc., __F. Supp. 3d__, 2017 WL 398657, at *3 (S.D.N.Y. Jan. 30, 2017) (citations omitted).[4]

1. Plaintiff Does Not Allege An Injury In Fact

---

[3] All internal quotations and citations are omitted unless otherwise noted.

[4] As set forth in defendants' concurrently filed motion to transfer, this case should be transferred to the Southern District of New York pursuant to the forum-selection clause in the Terms of Use Agreement that plaintiff Jason Cooper agreed to when he created his Unrollme account. *See* Motion to Transfer at 5. Because plaintiff agreed to litigate his claims in federal court in New York, Second Circuit law applies to plaintiff's claims. *Atlantic Marine Const. Co. v. U.S. Dist. Ct. for the W. Dist. of Tex.*, 134 S. Ct. 568, 583 (2013) (holding that "[t]he court in the contractually selected venue should not apply the law of the transferor venue to which the parties waived their right").

Plaintiff does not and cannot allege any facts demonstrating that he suffered any concrete or particularized harm caused by using Unrollme's services. First, plaintiff admits he authorized access to his Gmail account and does not allege facts showing he was actually harmed by defendants' alleged "mining" of his emails and the purported concerns that anonymized data can be re-personalized are simply hypothetical. Compl. ¶¶ 35, 38. Second, plaintiff does not dispute that access to user emails is necessary for Unrollme to perform its unsubscription services (which plaintiff concedes was authorized), or that Unrollme's free service is beneficial to users. *See id.* ¶¶ 20-23.[5] Third, Unrollme's purported failure to "adequately" inform users that defendants were collecting data from users' emails to develop anonymized market research products is undermined by the actual disclosures in Unrollme's Privacy Policy which plaintiff assented to.[6] *See id.* ¶ 28. But even assuming that the privacy disclosures were inadequate, plaintiff's allegations at most establish only an alleged procedural violation of a privacy interest, not an actual injury or even a likelihood that he has or will suffer any harm.

Simply alleging violation of a privacy interest without facts showing that plaintiff suffered an actual injury is not enough to allow plaintiff to maintain suit in federal court. The Second Circuit, in *Whalen v. Michaels Stores, Inc.*, __F. App'x __, 2017 WL 1556116 (2d Cir. May 2, 2017), held that a plaintiff failed to establish an injury in fact based on the alleged theft of her credit card information due to a consumer data breach where the plaintiff had not suffered any economic harm. *Id.* at *1-2. Despite that there were subsequent fraudulent attempts to use plaintiff's credit card, the Second Circuit held that they did not cause any injury in fact because plaintiff did not allege that she was required to pay any fraudulent charges. *Id.* The court further held that the allegation that plaintiff "suffered additional damages based on the opportunity cost and value of time that [she] and the Class

[5] Plaintiff alleges that "[w]hile millions of Americans have come to rely on email as a primary form of communication for their business and personal lives, their inboxes are increasingly being bogged down with the over 260 billion spam emails and advertisements sent daily. Defendant UnrollMe sought to capitalize on these frustrations and, in 2011, was founded specifically to 'clean up your inbox.'" *Id.* ¶ 1.

[6] Users including plaintiff are required to assent to the Privacy Policy in order to use Unrollme's services. *See id.* ¶ 19 (Figure 3 confirms that the sign up process requires users to click "Continue" to "agree to the terms and privacy policy" which are hyperlinked).

have been forced to expend to monitor their financial and bank accounts" was not specific or personal enough to confer standing. *Id.* at *2. The plaintiff in *Whalen* lacked standing where there was no harm alleged beyond the mere statutory violation. *See also Cruper-Weinmann*, 2017 WL 398657 at *3-4 (holding that a plaintiff failed to allege standing to sue for an alleged violation of the Fair and Accurate Credit Transactions Act of 2003 ("FACTA") based on an unredacted credit card number on a customer receipt, where the plaintiff did not allege that "any third party ever saw or accessed the receipt" or any facts "demonstrating that the violation in question put her at an increased risk of identity theft").

In *Gaos v. Google, Inc.*, No C 10-04809 JW, 2011 WL 7295480 (N.D. Cal. Apr. 7, 2011), the court held that a plaintiff had failed to establish Article III standing based on Google's alleged disclosure of her search queries in violation of the SCA, because her "conclusory allegations of disclosures of communications resulting in unspecified harm in violation of the ECPA, not supported by any facts, are insufficient to allege violation of Plaintiff's statutory rights." *Gaos*, 2011 WL 7295480, at *3; *see also Low v. LinkedIn Corp.*, No. 11-CV-01468-LHK, 2011 WL 5509848, at *3-4 (N.D. Cal. Nov. 11, 2011) (plaintiff lacked standing to sue for the alleged disclosure of his anonymous LinkedIn ID and browsing history, notwithstanding allegations that the disclosure caused him embarrassment and humiliation, because the plaintiff did not allege that "his browsing history, with embarrassing details of his personal browsing patterns, was actually linked to his identity by LinkedIn and actually transmitted to any third parties," nor had he alleged "*how* third party advertisers would be able to infer Low's personal identity from LinkedIn's anonymous user ID combined with his browsing history").

Similarly, in *Vigil v. Take-Two Interactive Software, Inc.*, __F. Supp. 3d__, 2017 WL 398404 (S.D.N.Y. Jan. 30, 2017), the court held that players of Take-Two's NBA 2K15 video game, which scans players' faces, did not have standing to sue for alleged violations of the Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. § 14/1, *et seq.* ("BIPA"), which was intended to protect against potential misuse of biometric data. *Id.* at *8. The plaintiffs alleged that Take-Two failed to comply with BIPA's provisions regulating the storage and dissemination of biometric information and requiring notice and consent to the collection of biometric information. *Id.* The court held that

these "procedural violations" were not sufficient to confer standing where plaintiffs failed to allege any use of their alleged biometric information beyond what was contemplated by the NBA 2K15 video game: "The creation of personalized basketball avatars for in-game play." *Id.* Moreover, the court found that plaintiffs alleged that they "received advance notice that their faces would be scanned, that they consented to have their faces scanned," and a "more extensive notice and consent could not have altered the standing equation because there has been no material risk of harm to a concrete BIPA interest that more extensive notice and consent would have avoided." *Id.* at *10-11.

As in *Whalen*, *Gaos*, and *Low*, the plaintiff in this case has not alleged any economic harm, and the generalization that "consumers who registered for Unrollme's email 'management service' had their privacy and trust violated" (Compl. ¶ 34) is insufficient to confer standing absent actual harm. Here, plaintiff admits he signed up and authorized Unrollme access to his inbox to "read" and "manage" his emails. *See* Compl. ¶¶ 20, 35. Unrollme's Privacy Policy further states that Unrollme "may disclose, distribute, transfer, and sell such [commercial and transactional] messages and the data that we collect from or in connection with such messages" provided that all personal information will be removed. *Id.* ¶ 28. While plaintiff alleges he "did not know that Defendants would actually use the access that UnrollMe acquired to read the contents of his emails and then sell that email to third parties," that challenged practice was specifically disclosed in the Privacy Policy *Id.* ¶¶ 28, 35. Plaintiff also does not allege that personal information was disclosed, and only alleges the abstract theoretical possibility that aggregated anonymized data can be re-identified. *See id.* ¶ 31. Similar to the facts in *Vigil*, plaintiff has not alleged that defendants did anything beyond "what was contemplated by" Unrollme's Privacy Policy, which plaintiff and users agreed to. *Vigil*, 2017 WL 398404, at *8. Also as in *Vigil*, plaintiff does not allege that he would not have used Unrollme's free email management service had he known that defendants would be extracting anonymized data from his transactional emails to develop market research products. *Id.* at *12. Accordingly, plaintiff has alleged only procedural violations, but not any material risk of harm to the interests that Congress intended to protect in the Wiretap Act and SCA. *See* S. Rep. No. 99-541, 1-3 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3555-57 (setting forth the purpose of the Wiretap Act and SCA as protecting "electronic communications" and "privacy interests in personal and proprietary

information"); *Cruper-Weinmann*, 2017 WL 298657, at *4 ("[T]here still must be some showing that the violation of the right actually threatened the harm in question if the plaintiff is to have standing."). His allegations cannot confer Article III standing.

2. Any Potential Future Harm That Plaintiff Alleges Is Purely Speculative

Nor can plaintiff remedy his failure to allege any actual harm by relying on hypothetical assertions that anonymized data sold by defendants can be re-personalized by a third party at some point in the future. Plaintiff, quoting from Unrollme's Privacy Policy, admits that any messages or data that Unrollme discloses, distributes, transfers, or sells is devoid of "all personal information contained in such messages." Compl. ¶ 28. Plaintiff does not allege that Unrollme failed to comply with this policy. Rather, he *hypothesizes* that Unrollme's anonymization of his messages and data "likely wasn't sufficient," because a third party may have the desire and ability to re-personalize his information. Compl. ¶¶ 31, 33. But plaintiff does not allege that any of his email messages were in-fact re-personalized, and any "possible future injury" that plaintiff contends may result from an "independent decisionmaker['s]" use of his anonymous messages and data is "not certainly impending" and does not create standing. *Clapper*, 133 S. Ct. at 1147-48 ("[T]hreatened injury must be certainly impending to constitute injury in fact, and [] allegations of possible future injury are not sufficient.").

"In *Clapper*, the [Supreme] Court emphasized that, to establish Article III standing, a future injury must be 'certainly impending,' rather than simply speculative. . . . [A] 'theory of standing[ ] which relies on a highly attenuated chain of possibilities[ ] does not satisfy the requirement that threatened injury must be certainly impending.'" *Whalen*, 2017 WL 156116, at *1 (quoting *Clapper*, 133 S. Ct. at 1148) (holding that a plaintiff whose credit card had been allegedly stolen and third-parties had attempted to use it for fraudulent purchases did not allege "how she can plausibly face a threat of future fraud, because her stolen credit card was promptly canceled after the breach and no other personally identifying information" was stolen); *see also Antman v. Uber Techs., Inc.*, No. 3:15-cv-01175-LB, 2015 WL 6123054 (N.D. Cal. Oct. 19, 2015) (Beeler, J.) (holding that alleged risk of identity theft based on data stolen from Uber was not "certainly impending" under *Clapper*, because the data breached included only the plaintiff's name and driver's license number that could

not, standing alone, be used to steal money or an identity). In *Vigil*, the court held that defendant's alleged statutory violation did not confer Article III standing because "there has been no event, such as [a] data theft . . . that could make any such risk rise above the abstract level." *Vigil*, 2017 WL 398404, at *9. Plaintiffs' allegations that the violations "subjected their face scans to an 'enhanced risk of harm' of somehow falling into the 'wrong hands'" was "too abstract and speculative to support standing," because the plaintiffs did not allege that their face scans had been obtained by a third party or otherwise stolen or misused in any way. *Id.*

Similarly, in *Fero v. Excellus Health Plan, Inc.*, __F. Supp. 3d__, No. 6:15-CV-06569 EAW, 2017 WL 713660 (W.D.N.Y. 2017), the court held that plaintiffs whose personal data had been compromised in a data breach did not establish Article III standing based on the "alleged increased risk of harm" resulting from the breach. *Fero*, 2017 WL 713660, at *10. "While they all allege that their personal information was compromised as a result of the data breach . . . none allege any facts indicating other suspicious activity has occurred in the three years since the data breach began." *Id.* The plaintiffs' failure to identify any actual harm "undercuts their assertion that the asserted harm of future identity theft is 'certainly impending,'" because any alleged injuries "rely on a chain of possibilities about the actions of independent actors:" (1) the plaintiffs "may suffer some actual harm if the hacker has the information in a format that is understandable and accessible"; (2) "and if the hacker intends to commit crimes by misusing it or transmitting it to someone who does," and (3) "if the hacker (or other party) can successfully misuse the information." *Id.*[7]

Here, plaintiff's alleged concerns that anonymized data can be re-identified are too theoretical

[7] Other courts have similarly held that an alleged risk of future harm premised upon a series of assumptions regarding the conduct of unknown third-parties is too speculative to confer standing. *See Attias v. CareFirst, Inc.*, 199 F. Supp. 3d 193, 200 (D.D.C. 2016) (alleged increased risk of identity theft from breach of insurance policyholders' personal information not "certainly impending" because court "would have to assume, at a minimum, that the hackers have the ability to read and understand Plaintiffs' personal information, the intent to commit future criminal acts by misusing the information, and the ability to use such information to the detriment of [Plaintiffs]"); *Cahen v. Toyota Motor Corp.*, 147 F. Supp. 3d 955, 973 (N.D. Cal. 2015) (alleged "risk of future identity theft" based on Toyota Motor Corp.'s collection of the geographic location and transmission of that information to a third party by an insecure software was not "certainly impending" because it was "not apparent how the purposeful disclosure of such data to a third party [] would establish any credible risk of future harm," and the plaintiffs had not alleged any "breach or data compromise").

and attenuated to establish standing. Plaintiff's allegation that Uber is the type of company that would attempt to de-anonymize data is completely speculative, and not tied in any way to plaintiff's use of Unrollme's services (plaintiff does not even allege that he is a Lyft user or had his anonymized email data sold to Uber).

B. Plaintiff's Claims Should Be Dismissed Under Fed. R. Civ. Proc. 12(b)(6)[8]

1. Plaintiff Cannot State A Claim Under The Wiretap Act Or SCA Because Unrollme Is A Party And/Or Intended Recipient Of His Messages

By signing up to use Unrollme's email management services, the plaintiff gave Unrollme access to his emails, making Unrollme a party to and intended recipient of his communications. The plaintiff, therefore, cannot state a claim under the Wiretap Act or the SCA, because both statutes exclude a "party" to a communication, or conduct authorized by an intended recipient of the communication, from liability. The Wiretap Act excludes an interception by a "party to the communication or where one of the parties to the communication has given prior consent to such interception" from liability. 18 U.S.C. § 2511(2)(d). The SCA excludes from liability the access of a stored electronic communication when "authorized" "by a user of [an electronic communication service] with respect to a communication of or intended for that user." 18 U.S.C. § 2701(c)(2). An "electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system . . . ." 18 U.S.C. § 2510(12).

In the context of content delivered via the Internet, courts have held that parties to a communication include intended recipients of transmissions of data via servers, web browsers, and

[8] A complaint will only survive a Rule 12(b)(6) motion to dismiss if it alleges "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). While in evaluating a motion to dismiss, the court must assume that the plaintiff's factual allegations are true but the court must not "accept as true a legal conclusion couched as a factual allegation." *Twombly*, 550 U.S. at 555. The "plaintiff's obligation to provide the 'grounds' of his 'entitle[ment] to relief' requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do . . . . Factual allegations must be enough to raise a right to relief above the speculative level . . . ." *Id.* at 555. "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). But where the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct, the complaint has alleged—but it has not 'show[n]'—'that the pleader is entitled to relief.'" *Iqbal*, 556 U.S. at 679.

websites. *See, e.g.*, *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 142-43 (3d Cir. 2015) (ruling that under section 2511(2)(d) Google was exempt from liability because Google was a party to transmissions containing internet usage information in cookie files through its operation of servers that served advertisements to plaintiffs' personal web browsers, notwithstanding allegations that Google "induced" plaintiffs to "voluntarily" communicate with it "by deceit" by "surreptitious circumvention of the cookie blockers")), *cert. denied sub nom. Gourley v. Google, Inc.*, 137 S. Ct. 36 (2016). Where a defendant is found to be a party to the communication, liability does not attach where 1) a plaintiff or user did not intend to allow a corporate defendant to intercept or access electronic communications, or 2) access was provided by a website to a third party without the individual plaintiff/website user's knowledge or permission. *See id.*; *Caro v. Weintraub*, 618 F.3d 94, 97-98 (2d Cir. 2010) ("In the context of the statute, a party to the conversation is one who takes part in the conversation . . . we can find . . . no support for the proposition that one must be invited to a conversation in order to be a party to it" under section 2511(2)(d)); *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 510-11 (S.D.N.Y. 2001) (plaintiffs' "naked allegation that the defendant's access was unauthorized" could not support SCA claim where their communications were "'intended for'" the defendant's "affiliated Web sites who have authorized [the defendant's] access" under section 2701(c)(2)).

For example, in *In re Google*, the Third Circuit held that Google was not liable because it was a party to plaintiffs' communications with third-party websites, despite allegations that Google circumvented cookie blockers and obtained the information by "deceit," where plaintiffs' browsers requested Google to deliver content from its servers and in that process acquired the plaintiffs' internet history information. *In re Google*, 806 F.3d at 140-43. The plaintiffs alleged that they implemented cookie blockers to stop Google from placing cookies that tracked the websites they visited, and relied on Google's public statements assuring users that the cookie blockers could "refuse all cookies" or "block all third party cookies." *Id.* at 132-34. Notwithstanding that Google circumvented the cookie blockers, the Third Circuit held that Google was not liable under the Wiretap Act because Google could only intercept the communications with a cookie if the plaintiffs directed their browsers to a web page that displayed advertisements from Google, thereby requesting

Google to display the relevant advertising and making Google a party to the communication. *Id.* at 140-41. The court also rejected plaintiffs' claims that Google became a party to the communications through "deceit," because "[t]here is no statutory language indicating [that section 2511(2)(d)] . . . excludes intended recipients who procured their entrance to a conversation through fraud in the inducement, such as, here, by deceiving the plaintiffs' browsers into thinking the cookie-setting entity was a first-party website," and therefore denied holding Google liable for "equitable reasons." *Id.* at 143; *see also Caro*, 618 F.3d at 97-98 (holding that third party that allegedly overheard and recorded a plaintiff's conversations without permission was a party to the communications because he was present with the plaintiff when the conversations occurred, despite the plaintiff's contention that he did not invite the third party to participate in the conversation).

Similarly, in *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262 (3d Cir. 2016) *cert. denied sub nom. C.A.F. v. Viacom Inc.,* 137 S. Ct. 624 (2017), Google was held not liable under the Wiretap Act for allegedly tracking the plaintiffs' web-browsing history with cookies placed on the computers belonging to visitors of Viacom websites, because Google's cookies either made it a party to plaintiffs' communications, or Google's conduct was exempt under section 2511(d)(2) because Viacom, the operator of the website, authorized it. The plaintiffs alleged that, without their consent, Viacom placed cookies on their computers when they visited Viacom's websites, and Viacom allowed Google to place cookies on the computers as well. *Id.* at 269. The Third Circuit held that Viacom was a party to the communications because they occurred on Viacom's website, and "Google was either a party to all communications with the plaintiffs' computers," or, Google was not liable under the Wiretap Act because it "was permitted to communicate with the plaintiffs' computers by Viacom, who was itself a party to all such communications." under section 2511(d)(2). *Id.* at 274.

Courts applying the intended recipient exception under section 2701 of the SCA have similarly held that as long as one party to a communication authorizes access to that communication while in storage, no liability attaches under the SCA. For example, in *In re DoubleClick*, the court held that plaintiffs failed to state a claim against an internet advertisement service under the SCA for allegedly accessing the plaintiffs' communications with the websites that they visited because the *websites* authorized the access when it hired the service to sell targeted advertisements based on user

demographics. *In re DoubleClick*, 154 F. Supp. 2d at 510-11.[9] And in *In re American Airlines, Inc. Privacy Litigation*, 370 F. Supp. 2d 552 (N.D. Tex. 2005), the court held that plaintiffs, American Airlines passengers, who alleged that a third party had accessed their records with American Airlines without their consent, failed to state a claim against the third party under the SCA because *American Airlines* had authorized the access. *Id.* at 558.

2. Cooper Does Not Allege A Plausible "Interception" Under The Wiretap Act

To state a claim under the Wiretap Act, Cooper must allege that Unrollme and Slice "intercepted" his electronic communications. 18 U.S.C. § 2511. An "interception" under the Wiretap Act is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). An acquisition of an electronic communication is an interception under the Wiretap Act only if that acquisition occurs "contemporaneous with transmission" of the communication. *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 876-78 (9th Cir. 2002) ("in cases [dealing] with 'electronic communications'—the definition of which specifically includes 'transfer' and specifically excludes

[9] Moreover, even if Cooper had attempted to allege claims against Unrollme or Slice for unlawful disclosures under section 2702 of the SCA—which he has not—his claims would fare no better. The SCA also excludes from liability a disclosure "to an addressee or intended recipient of such communication" or "with the lawful consent of the originator or an addressee or intended recipient of such communication." 18 U.S.C. § 2702(b)(1), (3). In *American Airlines*, the court held that the plaintiffs failed to allege that American Airlines unlawfully disclosed their communications to a third party in violation of the SCA, because, even if the disclosure violated American Airlines' privacy policy, American Airlines had consented to the disclosure, and the privacy policy "did not deprive [American Airlines] of the legal capacity under § 2702(b)(3) to consent to disclosure." *American Airlines*, 370 F. Supp. 2d at 560-61. Similarly, in *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705 (N.D. Cal. 2011),) *aff'd*, 572 F. App'x 494 (9th Cir. 2014), the court held that plaintiffs failed to state a claim against Facebook based on Facebook's provision of information about its users to third-party advertisers that Facebook sent when users clicked on advertisements on Facebook's website, because Facebook, as the operator of the website through which plaintiffs communicated with the advertisers, was either the "addressee or intended recipient" of plaintiff's communications. *In re Facebook Privacy Litig.*, 791 F. Supp. 2d at 708-09, 713. That Facebook's disclosures contravened its policies did not make the disclosures actionable under the SCA. *In re Facebook Privacy Litig.*, 791 F. Supp. 2d at 708-09, 713 (the court applied a similar rationale to dismiss the plaintiffs' claims under the Wiretap Act); *see In re Zynga Privacy Litig.,* No. C 10-04680 JWW, 2011 WL 7479170, at *2 (N.D. Cal. June 15, 2011) (dismissing plaintiffs' Wiretap and Stored Communications Act claims where "the electronic communications in question were sent to Defendant itself, to Facebook, or to advertisers, but both Acts exempt addressees or intended recipients of electronic communications from liability for disclosing those communications"), *aff'd,* 750 F.3d 1098 (9th Cir. 2014).

'storage' . . . it is natural to except non-contemporaneous retrievals from the scope of the Wiretap Act") (citation omitted); *see also Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457, 461-62 (5th Cir. 1994) (analyzing language of Wiretap statute and concluding that "Congress did not intend for 'intercept' to apply to 'electronic communications' when those communications are in 'electronic storage.'"); *Hoyle v. Diamond*, No. 08-cv-347C, 2013 WL 1152037, at *10 (W.D.N.Y. Mar. 19, 2013) ("Courts addressing the meaning of 'intercept' narrowly define it to include only acquisitions of communication contemporaneous with transmission, not storage.") (collecting authorities).

Conversely, accessing electronic communications while they are stored in memory on a device or server, even if only for a fleeting moment, is not actionable under the Wiretap Act. *See Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197, 205 (2d Cir. 2016) (distinguishing between Title I of the Electronic Communications Privacy Act, the Wiretap Act, which "appl[ies] to interception of computer and other digital and electronic communications" from the SCA, which applies to communications stored in a web-based e-mail account); *Theofel v. Farey-Jones*, 359 F.3d 1066, 1077-78 (9th Cir. 2004) (unauthorized access to stored emails does not violate the Wiretap Act); *Konop*, 302 F.3d at 877 (holding no interception occurred in violation of Wiretap Act when employer gained unauthorized access to secure website maintained by employee containing bulletins critical of employer because employer acquired website's contents in their stored state, and not during transmission); *Mintz v. Mark Bartelstein & Assocs. Inc.*, 906 F. Supp. 2d 1017, 1031 (C.D. Cal. 2012) (dismissing Wiretap Act claim where "Defendants did not access, disclose, or use any emails that had been acquired during transmission[;]" "[r]ather, the emails Defendants viewed were stored on Gmail").

The complaint alleges no facts whatsoever to show that either Unrollme or Slice "intercepted" plaintiff's emails "*contemporaneous* with transmission" of those emails. Rather, plaintiff alleges that when users sign up for Unrollme's free service, users "grant[] it access to their private email inbox," which contains stored electronic communications. Compl. ¶ 17; *see also id.* ¶ 29 (users give Unrollme "access to users' email accounts"), ¶ 38 (defendants "accessed his emails, read the contents of those emails"). Because the Wiretap Act does not apply to communications in storage, plaintiff cannot state a claim under Title I of ECPA.

IV. CONCLUSION

For the foregoing reasons, plaintiff's claims are subject to dismissal in their entirety pursuant to Fed. R. Civ. Proc. 12(b)(1) because plaintiff failed to allege an injury in fact, where the mere alleged abstract possibility that anonymized data allegedly extracted from his emails and aggregated with other data could be potentially de-anonymized, is too hypothetical and speculative to confer standing to establish Article III jurisdiction. Additionally, plaintiff's claims are subject to dismissal in their entirety pursuant to Fed. R. Civ. P. 12(b)(6) because Unrollme was either a party or intended recipient of plaintiff's electronic communications and therefore the alleged access to his communications is not actionable under ECPA. Plaintiff's claim under the Wiretap Act is subject to dismissal for the additional reason that he has failed to allege a plausible interception by any defendant. Under either Rule 12(b)(1) or 12(b)(6), or both, the Court should grant defendants' motion and dismiss the plaintiff's claims in their entirety, with prejudice.

Respectfully submitted,

DATED: June 19, 2017

GREENBERG TRAURIG, LLP

By: */s/ Ian C. Ballon*
Ian C. Ballon
Lori Chang
Rebekah S. Guyon

Attorneys for defendants Slice Technologies, Inc. and Unrollme Inc.